NATNetwork Address Translation

What is NAT

NAT 定義於 RFC 2663, RFC3022, 基本上它是在 router 中進行一個偷換 IP header 的動作, 以便讓多台電腦能共用一個 IP 連上 Internet 的技術. 許多的 router 目前有都有支援 NAT 這項功能, 其它如 Linux 中的 IP Masquerade, FreeBSD 中的 NATD, 或是 Win95 上的 Sygate 軟體也是指一樣的東西.

NAT 一般多配合 Private IP Address 一同使用

NAT 的優點

由於對外只使用一個 IP address, 因此內部使用的 IP 可重覆地在不同單位使用

只要少數 public address 就能讓單位內所有電腦都連上 Internet

只有使用 public address 的電腦會被單位外部網路所存取, 使用 private address 的電腦不會直接被存取, 有安全上的好處

格式化: 字型: (中文) 標楷體, 16 點, 粗體

格式化: 置中

格式化

格式化

格式化

格式化

格式化

~~NAT 的缺點~~

~~通訊協定資料中如含有其 IP address 者將無法使用~~

~~(一般的 NAT 實作會修改出現在 FTP 和 ICMP 通訊協定~~

~~資料中的 IP address, 但其它協定就不管了)~~

~~以 IP address 作為安全檢查的方式將不可行~~

~~Private IP Address~~

~~Why Private IP Address~~

~~為了解決 IP 日漸不足的問題, RFC1918 中定義了一段~~

~~Private IP address, 這段 IP 可作為企業或單位內自行運用~~

~~的 IP Address 而無須經過向上游申請的手續.當然使用單位~~

~~必須負責不讓這些 Private IP Address 的 routing~~

~~information 流到單位外的網路上, 也就是說這些電腦只能~~

~~和單位內的電腦連線, 外面的網路看不見單位內這些~~

~~Private IP Address 的電腦, 因此這段 Private IP Address~~

~~可重覆地被不同單位內部所使用, 進而達到節省 IP 的目的.~~

~~什麼是 NAT 與 DHCP 協定介紹~~

格式化 ...

格式化 ...

格式化 ...

格式化 ...

格式化: 字型: (中文) 標楷體, 16 點, 粗體

格式化 ...

NAT (Network Address Translation) 可以讓你區域網路中的所有機器經由一台通往 Internet 的 server 連線出去，而且只需要一個真實 IP 就可以了。

Private IP Range
RFC 1918 共定義了三個範圍的 Private IP address

Addr Range	mask
10.0.0.0 - 10.255.255.255	10.0.0.0/255.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0/255.240.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0/255.255.255.0

程榮祥
Email: rscheng@mail.ksu.edu.tw

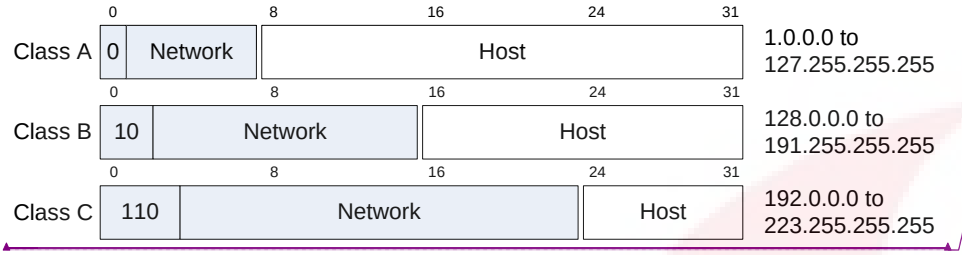
Private IP 優點
節省 IP 的使用
讓網路設計時能有較大的彈性

Pricate IP 缺點
使用 Private IP 的電腦無法連上 Internet

Classful 定址與 IPv4 CIDR

網際網路原始的定址架構，依功能與範圍可分為 A、B、C、D、E 五個 Class，其中 A、B、C 作為一般用途使用，D 是群播位址，而 E 則保留作為實驗網路使用。IP 位址可分成 Network 與 Host 兩個部份，Network 代表所屬的網段，網段中的電腦主機則用 Host 來識別。例如，以 Class A 的位址來說，前面 8 個位元用來識別網段，後面 24 位元用來識別網路中的電腦。Class B 使用前面 16 個位元來識別網段，後面 16 位元則用來識別網路中的電腦；最後，Class C 則是使用前面 24 個位元來識別網段，後面 8 位元用來識別網路中的電腦。Class A、B、C 的定址空間如下圖所示:

《網路新知》



這種單純的以 Class 來區分所屬網段及主機名稱的定址方式，有時候又稱之為 Classful addressing。實際上，網際網路已經不再正式採用這樣的架構作為標準了。因為以一個有 5,500 台電腦主機的單位而言，如果想申請一個網段給這個單位內部的電腦使用，那麼就需分配一個 Class B 給它 (可定址 65,534 個主機位址)，但事實上，這樣的分配遠超出它的需求，~~因此~~這個網址在被分配出去之後，它會留下超過 60,000 個位址沒有使用，並且也不能讓其它機構使用。因此，可以預見的，以這種方式來分配 IP，將會讓可用的 IP 位址空間快速地耗盡。

~~Network Address Translation　網路位址轉換路由器：NAT Router~~

~~作者:蔣大偉~~

~~前言~~

~~最近幾年來由於網路節點的使用快速成長的普及化，使得網際網路傳輸協定~~

~~IPv4IP 位址逐漸地不符不敷使用。其原因有三：為了疏為此緩 IP 不足的問題，於是~~IETF 在 1993 年訂定 Classless interdomain routing (CIDR) 標準，將網路的地址方式由原先的 Classful addressing 的定址方式改以 domain/mask 的方式代替；例如以 212.2.4.0/24 這個網段來說，其中"/24"這個符號代表 32 位元 IP 位址最左邊的 24 位元為網段位址，這些用來定址網段的最左邊位元，有時候也稱為網路前置位元 (network prefix)。~~將網路的地址方式由原先的 Classful addressing 改由 IP 位址再加上 network prefix 來代替。Prefix 的長度就代表~~

~~1.B 等級位址範圍已全部釋出；~~

~~2.所有位址空間終將用完；~~

~~3.路由器的路徑表太大導致骨幹路由器無法負荷。IP 位址的 network domain。因此~~使用 CIDR 的方式來地址之後，IP 位址的網~~路~~段部份可以包含任意長度的位元數，而不一定要限制使用 8、16 或 24 位元。

格式化
格式化: 左右對齊, 縮排: 第一行: 0.85 cm
格式化
格式化: 左右對齊
格式化
格式化
格式化
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化
格式化
格式化
格式化
格式化
格式化: 左右對齊

Private IP Address

為了解決 IP 日漸不足的問題，在 RFC 1918 中也定義了一段 Private IP address，可以讓機關組織，或是一般的使用者在區域網路內部能自行運用而無須向 ISP 或管理網域位址管理網域位址的的單位提出申請。當然使用單位必須負責不讓這些 Private IP address 的路由資訊 (Routing information) 不能在網路上被傳送，因此流到單位外的網路上。使用 Private IP address 的電腦只能和區域網路內部的其它電腦連線。由於外部的網路看不見這些使用 Private IP address 的電腦，因此所以這些 Private IP address 可重覆地被不同單位在被不同單位的區域網路內部所使用，進而達到節省 IP 的目的。

RFC 1918 共定義了三個範圍的 Private IP address，如下表所示：

Network/Mask	數量
10.0.0.0/255.0.0.0	1 個 Class A
172.16.0.0/255.240.0.0	16 個 Class B
192.168.0.0/255.255.255.0	255 個 Class C

儘管使用 CIDR 及 Private IP 定址的方式可以暫緩 IP 不足的問題，但是隨著網路的普及，各種應用對於 IP 位址的使用也需求也愈來愈大。為了因應大量 IP 的需求，因此 IETF 也開始致力於開發 IPv4 協定的後續版本－IPv6。IPv6 有 128 位元的定址空間，可解決 IP 不足的問題並提供更多的服務。不過由於目前的網路設備都是使用 IPv4，要將網路的定址方式由 IPv4 逐漸轉移到 IPv6 需要一段很長的時間，因此 IPv6 被視為是一種長期的解決方案。在 IPv6 尚未普及之前，而 CIDR IPv4 又無法提供大量 IP 需求時，另一個過渡時期的解決方案則逐漸地廣為使用，也就是接下來要介紹的－Network address translation 的方法。

Network Address Translation 網路位址轉換 (NAT)

由於近年來，由於使用網路的普及化使用人口快速增加，從大型企業到個人使用者，有愈來愈多電腦設備經由區域網路連上 Internet，如個人電腦、Notebook、PDA 等。由於區域網路內連上網路的電腦設備愈來愈多，在可用的 IP 位址空間有限的情況下，最簡單解決的地方法之一，就是允許多人可以同時共用有限的 IP。

Network Address Translation (NAT) 是一種允許許多台電腦主機能可以共用 IP 位址的技術。NAT 定義於 RFC 2663、RFC3022。NAT 的主要觀念是，在

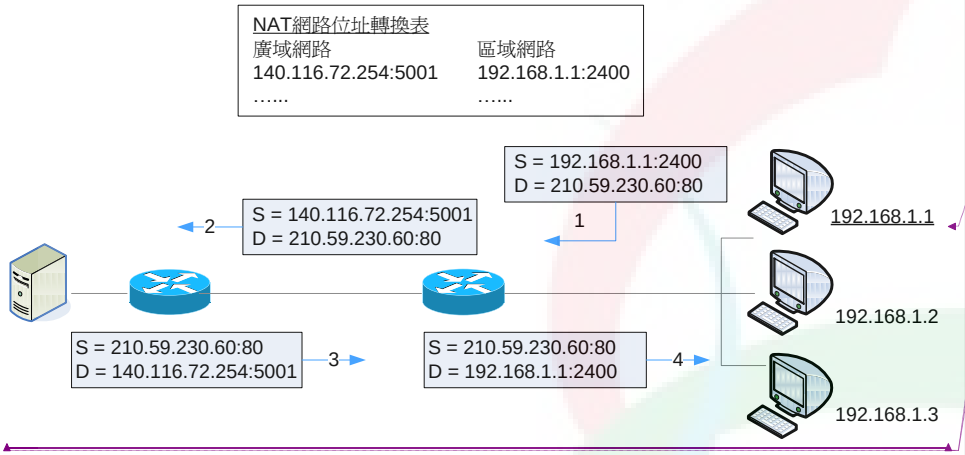
當電腦需要存取連線到外面部的網際網路時，

，才將區域網路內部使用的 Private 私有的 IP 位址轉換成正式的 IP 位址，並將轉換的 IP 和 Port 記錄於 NAT 路由器的網路位址轉換表 (NAT translation table)。相反地，因為同一時間連上

網際網路的電腦個數將會低於所有內部網路的電腦總數，當回傳的資料

格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化表格
格式化 ...
格式化 ...
格式化 ...
格式化 ...
格式化: 左右對齊
格式化 ...
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化 ...
格式化 ...
格式化: 字型: (中文) 標楷體

到達 NAT 路由器時，再利用網路位址轉換表取得正確的 IP 和 Port 將正式的 IP 位址動態地分配給需要用到的電腦，結束後再收回，可達到節省位址空間的目的。並將資料轉送給目的地主機。NAT 的運作方式如下圖所示：



NAT 在近幾年來已經很普遍地被使用，目前很多的路由器或是伺服器都有支援 NAT 的功能。

以下將說明 IPv4 所發生之困境、相關之衍生問題及有效解決方案等。而重點將放在較常用的解決方案是使用 NAT（Network Address Translation）Router 上。

NAT 的主要優點在於只需少量的 IP 位址就能讓單位內所有電腦都連上網際路，另外，由於使用 Private IP address 的電腦被隱藏在 NAT 內部，所以能提高內部主機的安全性；但缺點則是由於主機與主機之間無法直接進行通訊，若是需要這樣的服務則必需有其它替代方案來解決。另外，由於封包在出/入內部網段之前，都必須做 IP 位址的轉換，會增加許多的負擔，因此在使用 NAT 時也需要考慮提供 NAT 服務的網路設備是否能負荷。

IPv4 之 A、B、C 三等級

IPv4 的位址欄位長度為 32 個位元，共分為 A、B、C 三個等級，如下：

等級	網路組數	網路範圍
A	7bits=27=128 組	0-127.xx.xx.xx

格式化: 字型: (中文) 標楷體
格式化: 置中
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化: 左右對齊
格式化
...

B　14bits=214=16384 組　128-191.0-254.xx.xx

C　21bits=221=2097152 組　192-223.0-254.0-254.xx

路由器的 NAT 設定　由於其 B 等級位址的範圍都已分配出去，一旦等到 B 等級位址空間用完，勢必造成 C 等級位址的大量釋出，而導致所有位址空間終將用完。同時也因為路徑表太大，造成骨幹路由器無法負荷之結果。

為解決上述問題，我們可以用 CIDR（Classless Inter-Domain Routing）的方法減緩 B 等級位址空間被用完的速度。而要有效延後位址空間被用完的時間，除非增加 IPv4 的位址欄位長度，而路徑表太大導致骨幹路由器無法負荷，則可由 BGP-4 暫時解決。雖然 IPv4 似乎還能繼續存活，但是未來還是不得不走向下一代網際網路傳輸協定 IPv6。

解決方案一：IP Masqerade

由於無法增加 IPv4 的位址欄位長度，遂有許多其他的替代方案，用以節省位址空間的使用。其中一個解決方案是為 IP Masqerade，也就是在自己的內部網路使用私有位址空間，再透過 proxy 與網際網路連接。此雖然僅限於部份的應用或協定，但是整個內部網路只需一個與網際網路連接的 IP 位址即可，如此一來，將可大為節省網路位址空間的使用。

私有位址空間的範圍如下：在 RFC1597 中網際網路上負責分配 IP 位址的 IANA（Internet Assigned Number Authority）將下面三段 IP 位址空間保留給私有網路使用：

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

以上三段私有 IP 位址空間只允許用於內部私有網路中，故對外不必註冊。

解決方案二：NAT Router

較常用的解決方案是使用 NAT（Network Address Translation）

格式化

格式化: 字型: (中文) 標楷體, 粗體

Router 來動態分配正式的 IP 位址。當電腦連線到外面的網際網路時，才將內部私有的 IP 位址轉換成正式的 IP 位址。因為同一時間連上網際網路的電腦個數將會低於所有內部網路的電腦總數，將正式的 IP 位址動態地分配給需要用到的電腦，結束後再收回，可達到節省位址空間的目的。

使用 NAT Router 幾乎與應用程式無關，因為它只在第三層（IP 協定層）運作處理。而 NAT Router 是如何來完成 IP 位址轉換的功能？一般說來分成靜態和動態二種方式，說明如下：

先定義 m 及 n 二個參數

m：需要被轉換的 IP 位址個數（私有的 IP 位址或舊的 IP 位址）
n：能夠被分配的 IP 位址個數（正式的 IP 位址或新的 IP 位址）

靜態 NAT 的定義為：

m:n Translation, m,n≧1and m =n (m,n is N)

也就是說私有的 IP 位址個數與正式的 IP 位址個數相同。

靜態 NAT 的實作很簡單，只要一行邏輯轉換公式即可完成：

new-ip-addr=new-network-id OR(old-ip-addr AND(NOT netmask))

例如，NAT Router 要將網路 192.168.1 上所有的 IP 位址轉換成網路 140.109.5 上所有相對應的 IP 位址，netmask 皆為 255.255.255.0，現在私有的 IP 位址 192.168.1.3 要轉換成正式的 IP 位址 140.109.5.3

old-ip-addr=192.168.1.3
= old-network-id+old-host-id
= 1100 0000 1010 1000 0000 0001 + 0000 0011 = 192 168 1 + 3
NOT netmask=0000 0000 0000 0000 0000 0000 1111 1111
AND
=0000 0000 0000 0000 0000 0000 0000 0011
new-network-id=1000 1100 0110 1101 0000 0101= 140 109 5

格式化 ...

~~OR~~

~~=1000 1100 0110 1101 0000 0101 + 0000 0011 = 140 109 5 + 3~~

~~= new-ip-addr = 140.109.5.3~~

~~動態 NAT 的定義為：~~

~~m:n Translation, m,n≧1 and m≧n (m,n is N)~~

~~也就是說，私有的 IP 位址個數大於正式的 IP 位址個數；或是雖然二者個數相同但是基於安全理由不希望使用靜態的對應方式。~~

~~在動態 NAT 的環境中能夠同時連通外界網路的機器個數受限於正式的 IP 位址個數，當所有正式的 IP 位址分配完畢之後，任何的 IP 位址轉換要求將會被 NAT Router 拒絕，並回傳 host unreachable 之 ICMP 封包。動態 NAT 之實作較靜態 NAT 複雜，因為它必需維護一個動態表格以便記錄私有 IP 位址與正式 IP 位址之對應關係。~~

~~例如，NAT Router 要將 B 等級網路 172.16 上所有的 IP 位址動態轉換成 C 等級網路 140.109.5 上的 IP 位址範圍。每次內部網路有機器要連通外部網路時，NAT Router 會從 140.109.5 上的 IP 位址範圍內動態取得尚未分配出去的 IP 位址，並記錄在動態表格中直到斷線。若是內部網路機器的資料已經存在動態表格中，就使用該筆資料作轉換。只要動態表格中存在某內部網路機器的資料，外部網路的人就可以利用其所對應之正式 IP 位址與該內部網路機器進行連線。~~

~~src 172.16.2.100 ->NAT Router ->src 140.109.5.20~~

~~dst 172.16.2.100<- NAT Router<- dst 140.109.5.20~~

~~動態表格~~

~~私有 IP 位址~~	~~正式 IP 位址~~
~~172.16.2.100~~	~~140.109.5.20~~

~~如前所述，當 m=n 時有些人基於安全上的考量使用動態 NAT。因為~~

格式化 ...

~~使用動態 NAT 之後位於外部網路的人無法正確取得內部網路機器的 IP 位址，因為它每次與外部網路連通的 IP 位址可能都不一樣。~~

在設定動態 NAT 時，需要先設定可供 NAT 使用的 IP 位址轉換範圍，所以先使用 ip nat pool 指令設定 IP 的起始、結束位址範圍。設好之後，接著使用存取列表 (Access-List) 設定允許存取 NAT 的位址範圍，最後再使用 ip nat inside source list 指令將 IP 位址範圍應用上來。指令格式請參考下面的範例：

```
ip nat pool <pool-name> <start-IP-address> <end-IP-address> netmask <net-mask>
access-list <acl-number> permit <address-to-match> <wildcard-bits>
ip nat inside source list <acl-number> pool <pool-name>
```

上面的設定完成後，只要再指定連接 NAT 內部網段以及外部網段的網路介面即可，指令格式如下：

```
interface <inside-interface>
ip address <ip-address> <net-mask>
ip nat inside
!
interface <outside-interface>
ip address <ip-address> <net-mask>
ip nat outside
```

以下是一個完整的設定範例：

```
hostname Router
enable password xxxx

interface FastEthernet0/0
 description "外部網路介面"
 ip address 140.116.72.96 255.255.255.0
 ip nat outside
 duplex auto
 speed 100

interface Serial0/1
 description "內部網路介面"
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
clock rate 56000

ip nat pool natpool 140.116.72.96 140.116.72.96 prefix-length 24
ip nat inside source list 1 pool natpool
ip classless
ip route 0.0.0.0 0.0.0.0 140.116.72.253
no ip http server
```

格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 貼齊格線
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體, 粗體
格式化: 字型: (中文) 標楷體

```
access-list 1 permit 10.10.10.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255

default-value exec-character-bits 8

line con 0
 logging synchronous
line vty 0 4
 password xxxx
 logging synchronous
 login
```

在這個例子中，我們允許 10.10.10.0/24 以及 192.168.1.0/24 網段的封包可以透過 NAT 傳送出去。

顯示 NAT 的統計資訊

設好 NAT 後，可使用 show ip nat statistics 指令快速地查看 NAT 設定的相關統計資訊。執行範例如下：

```
Router#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet0/0
Inside interfaces:
  Serial0/1
Hits: 34  Misses: 34
Expired translations: 34
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool natpool refcount 0
 pool natpool: netmask 255.255.255.0
        start 140.116.72.3 end 140.116.72.3
        type generic, total addresses 1, allocated 0 (0%), misses 0
```

其中 Outside interfaces 表示連結外部網段的網路介面，Inside interfaces 則是連接 NAT 內部網段的網路介面。在這個例子中，NAT pool 的名稱為 natpool，可供轉換的 IP 位址範圍由 140.116.72.3 到 140.116.72.3，總共只一個；也就說，所有要連到外部網段的電腦都共用同一個 IP 上網。

測試 NAT

若想測試 NAT 是否能運作，可找一台使用 private IP 的網路設備，用 ping 指令測試一下看是否能 ping 到外部網路。

```
Nethost#ping tw.yahoo.com
Sending 5, 100-byte ICMP Echos to 202.43.195.52, timeout is 2 seconds:
!!!!!
```

格式化: 不要貼齊格線
格式化 ...
格式化: 不要貼齊格線
格式化 ...
格式化: 字型: (英文)Times New Roman, (中文) 標楷體, 12 點
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 不要貼齊格線
格式化 ...
格式化: 不要貼齊格線
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 縮排: 第一行: 2 字元
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點
格式化: 不要貼齊格線
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點, 不加底線
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點

Success rate is 100 percent (5/5), round-trip min/avg/max = 172/180/200 ms

顯示動態 NAT 的轉換表

在設定好後，若想查看 NAT 的轉換情形可使用 show ip nat translations 指令。執行結果如下：

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 140.116.72.96:6219 192.168.0.1:6219 202.43.195.52:6219 202.43.195.52:6219
udp  140.116.72.96:49630 192.168.0.1:49630 140.116.72.14:53 140.116.72.14:53
icmp 140.116.72.96:8669 192.168.0.1:8669 202.43.195.52:8669 202.43.195.52:8669
```

清除 NAT 轉換表

在 NAT 執行的過程中，若需要重新啟動 NAT，可使用 clear ip nat translation * 指令，將先前的轉換表內容清除：(可先用 ? 號查看有那些參數可以使用)

```
Router#clear ip nat translation ?
  *          Delete all dynamic translations
  forced     Delete all dynamic translations (forcefully)
  inside     Inside addresses (and ports)
  outside    Outside addresses (and ports)
  tcp        Transmission Control Protocol
  udp        User Datagram Protocol
```

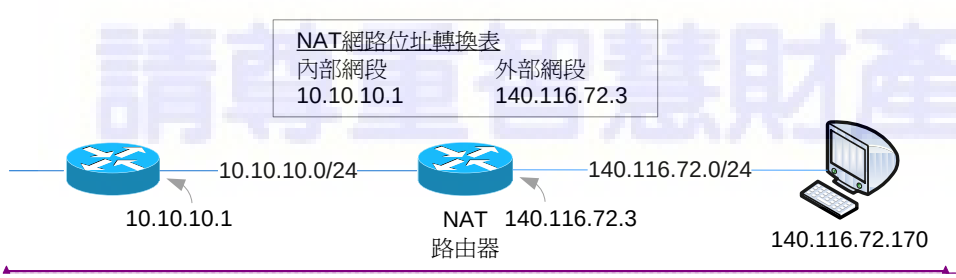
請執行 clear ip nat translation *指令，接著用 show ip nat translations 指令查看一下：

```
Router#clear ip nat translation *
Router#show ip nat translations
```

此時 NAT 轉換表的內容應該都是空的。

使用偵錯指令觀察 NAT 執行的情形

以下是我們實際去觀察在路由器中，NAT 執行的情形 (網路架構圖如下圖所示)。請執行 debug ip nat 指令，將偵錯模式打開：



格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點, 緊縮 0.4 pt
格式化: 不要貼齊格線
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點, 不加底線, 緊縮 0.4 pt
格式化 ...
格式化 ...
格式化 ...
格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化: 左右對齊
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點
格式化: 不要貼齊格線
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點, 義大利文 (義大利)
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 左右對齊
格式化 ...
格式化: 不要貼齊格線
格式化 ...
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點, 義大利文 (義大利)
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 左右對齊
格式化 ...
格式化 ...

```
Router#debug ip nat
IP NAT debugging is on
Router#
May 15 21:30:09: NAT: s=10.10.10.1->140.116.72.3, d=140.116.72.170 [310]
May 15 21:30:09: NAT*: s=140.116.72.170, d=140.116.72.3->10.10.10.1 [52693]
May 15 21:30:09: NAT: s=10.10.10.1->140.116.72.3, d=140.116.72.170 [311]
May 15 21:30:09: NAT*: s=140.116.72.170, d=140.116.72.3->10.10.10.1 [52694]
May 15 21:30:09: NAT: s=10.10.10.1->140.116.72.3, d=140.116.72.170 [312]
May 15 21:30:09: NAT*: s=140.116.72.170, d=140.116.72.3->10.10.10.1 [52695]
May 15 21:30:09: NAT: s=10.10.10.1->140.116.72.3, d=140.116.72.170 [313]
May 15 21:30:09: NAT*: s=140.116.72.170, d=140.116.72.3->10.10.10.1 [52696]
May 15 21:30:09: NAT: s=10.10.10.1->140.116.72.3, d=140.116.72.170 [314]
Router#
```

在這個例子中我們可以看到，來自 10.10.10.1 的封包在經過 NAT 時被來源端的 IP 位址轉換成 140.116.72.3 送出。目的端回傳的封包在經過 NAT 時，目的端的 IP 位址再被轉換成 10.10.10.1，經由路由器轉送到封包的目的地 IP 位址。相信在看過前的設定範例以及的解說後，讀者應該都很清楚 NAT 是怎麼運作的了。

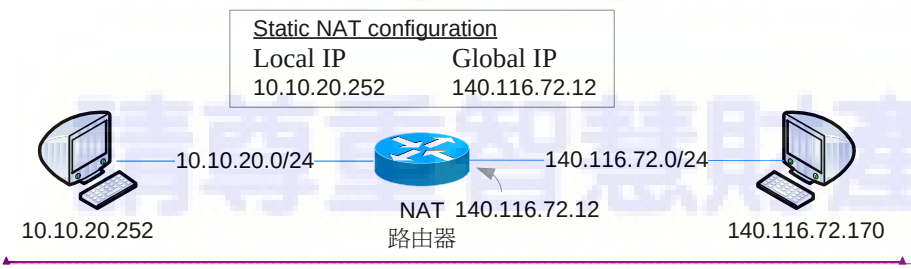
設定靜態 NAT (Static NAT)

NAT 除了使用動態轉換外，也可以用靜態轉換的方式直接將外部網段上的某個 IP 位址指定給 NAT 內部的某台電腦主機使用，這在需要能讓網際網路上的電腦能直與部份 NAT 內部的主機直接溝通時很有用。其指令語法如下：

ip nat inside source static *local-ip global-ip*

其中 *local-ip* 是指 Private IP 位址，*global-ip* 則是可在 Internet 上使用的 Global IP 位址。ip nat inside source static 指令可提供一對一的 NAT 轉換；當封包只需要在內部網段交換時，就使用 local-ip 位址；但是需通過 NAT 與外部網段進行資料交換時，則使用指定的 global-ip 位址。對於外部網段的電腦而言，與指定的 global-ip 交談，就等於與 local-ip 進行交談。

以下是實際的範例，(config)#為路由器提示符號：



設定靜態 NAT

Router(config)#ip nat inside source static 10.10.20.252 140.116.72.12

顯示 NAT 轉換表

Router#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	140.116.72.12	10.10.20.252	---	---

觀察 NAT 的執行情形

以上圖為例，我們可以使用 ping 指令先測試可否從外部網段 (主機 IP 位址：140.116.72.170) ping 到 NAT 內部的主機 (10.10.20.252)；其中 $ 為 Unix shell 提示符號：

```
$ ping 140.116.72.12
PING 140.116.72.12 (140.116.72.12) 56(84) bytes of data.
64 bytes from 140.116.72.12: icmp_seq=1 ttl=254 time=29.9 ms
64 bytes from 140.116.72.12: icmp_seq=2 ttl=254 time=29.2 ms
```

為了方便觀察，我們將路由器的偵錯模式打開，看看路由器收到 ping 的封包時會有什麼反應：

```
Router#debug ip nat
IP NAT debugging is on
Router#
May 17 22:33:59: NAT*: s=140.116.72.170, d=140.116.72.12->10.10.20.252 [0]
May 17 22:33:59: NAT*: s=10.10.20.252->140.116.72.12, d=140.116.72.170 [0]
Router#
May 17 22:34:00: NAT*: s=140.116.72.170, d=140.116.72.12->10.10.20.252 [0]
May 17 22:34:00: NAT*: s=10.10.20.252->140.116.72.12, d=140.116.72.170 [0]
Router#
```

從 debug 顯示的訊息可以看到，當外部主機去 ping 我們指定的 global-ip 位址時，NAT 會自動將目的位址轉換成 local-IP 位址，並將封包轉送給擁有 local-IP 位址的主機，反之亦然。在指定靜態 NAT 轉換時，最好也確定一下，路由器是否已經有路由可將封包送到指定的內部網段。

DHCP 協定

DHCP (Dynamic Host Configuration Protocol) 是一種動態指定主機 IP 位址的協定。DHCP 可以允許使用者在連上網路時，動態地從 DHCP 伺服器取得 IP 位址，並自動處理連上網路時相關的設定工作 (隨插即用：Plug-and-play)。由於 DHCP 可以提供在設定網路時的便利性，因此現在已經廣泛地被使用在區域網路以及無線網路中。

對於一個新加入網路的主機而言，DHCP 協定會進行以下四個步驟 (如下圖所示)：

格式化 ...
格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點
格式化: 不要貼齊格線
格式化 ...
格式化: 字型: (中文) 標楷體
格式化 ...
格式化: 字型: (中文) 標楷體
格式化: 左右對齊, 縮排: 第一行: 2 字元
格式化 ...
格式化: 不要貼齊格線
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 左右對齊
格式化 ...
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點
格式化: 不要貼齊格線
格式化 ...
格式化 ...
格式化 ...
格式化 ...
格式化: 字型: (英文)Verdana, (中文) 標楷體, 10 點
格式化: 字型: (中文) 標楷體
格式化: 字型: (中文) 標楷體
格式化: 左右對齊
格式化 ...

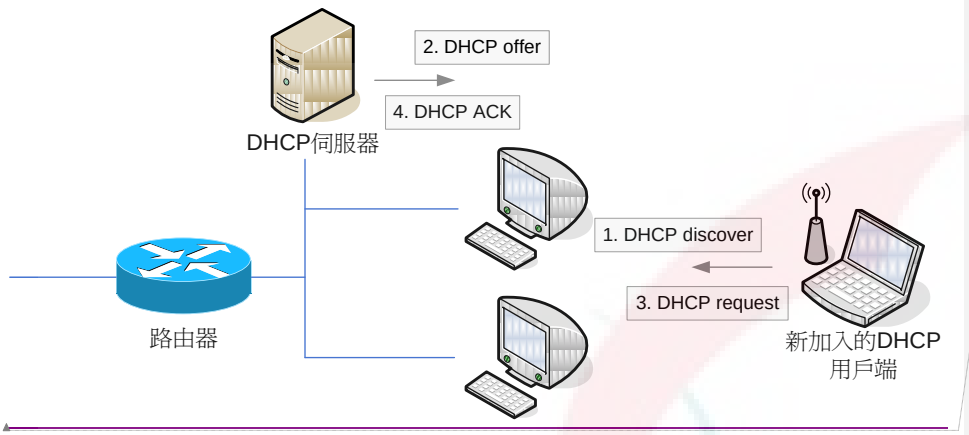


圖: DHCP 用戶端和伺服器的互動

1. 搜尋 DHCP 伺服器

對於使用自動取得 IP 方式連上網路的主機而言，它的第一個工作就是要找到可以與其互動的 DHCP 伺服器。由於尚未取得 IP 位址，因此 DHCP 的用戶端 (Client) 會使用廣播的方式送出一個 DHCP 搜尋訊息 (DHCP discover message)，其目的位址為 255.255.255.255，而來源位址則設為 0.0.0.0。網路上所有的電腦都會收到這個搜尋訊息，包括 DHCP 伺服器；在這個搜尋訊息中包含有一個協議識別碼 (Transaction ID) 以區分此訊息。

2. DHCP 伺服器提議訊息

接收到 DHCP 搜尋訊息的 DHCP 伺服器，會回應一個 DHCP 提議訊息 (DHCP offer message)，訊息中會包含先前收到的協議識別碼，建議用戶使用的 IP 位址、網路遮罩和 IP 位址的租約時間 (IP address lease time)；這個租約時間是指 IP 位址的合法使用時間。

3. DHCP 請求訊息

新加入的用戶可從多個 DHCP 提議訊息中加以選擇，然後送出 DHCP 請求訊息來回應所選擇的提議，同時也會回應組態設定參數。

4. DHCP 回應訊息

伺服器會利用 DHCP 回應訊息來回應 DHCP 請求訊息，並確認所請求的參數。

用戶端一旦接收到 DHCP 回應訊息，便完成與伺服器的互動，用戶端可以在租約期間內使用 DHCP 伺服器所分配的 IP 位址。因為用戶也有可能在租約到期後仍然想繼續使用 IP 位址，所以 DHCP 也提供用戶可以更新租用 IP 位址的機制。

設定 DHCP Pool

功能變數代碼變更

格式化: 項目符號及編號

格式化: 項目符號及編號

格式化: 項目符號及編號

格式化: 項目符號及編號

在路由器上設定 DHCP 時，步驟大致如下 (#為 CLI 提示符號)：

(1) 設定 DHCP 位址的 pool name 並進入 DHCP pool 設定模式

(2) 指定分配給使用者的網段範圍以及網路遮罩

(3) 指定 DHCP 用戶端的預設閘道位址

(4) 設定 DHCP 用戶端的網域名稱伺服器位址

(5) 指定租用的時間

格式化: 項目符號及編號

設定 DHCP 的指令格式如下：

```
Router(config)# ip dhcp pool name
Router(config-dhcp)# network network-number [mask | / prefix-length]
Router(config-dhcp)# default-router address
Router(config-dhcp)# dns-server address
Router(config-dhcp)# lease {days[ hours][ minutes] | infinite}
```

以下是一個設定的範例：

```
ip dhcp pool 10pool
   network 10.10.1.0 255.255.255.0
   default-router 10.10.1.254
   dns-server 140.116.72.14
```

在這個例子中，我們 DHCP 分配給使用者使用的網段範圍為 10.10.1.0/24，預設閘道為 10.10.1.254，網域名稱伺服器為 140.116.72.14；若沒有指定租用的時間，預設時間為 1 天。

Excluding IP Addresses

在使用上述指令設定 DHCP 後，只要使用者提出請求 DHCP 請求，DHCP 伺服器就會將 pool 中的 IP 分配出去。若在設定時，希望其中的某些網段不要分配出去，可以使用 ip dhcp excluded-address 指令，將之排除。指令格式如下：

```
Router(config)# ip dhcp excluded-address low-address [high-address]
```

顯示 DHCP 位址分配 (Address binding)

當我們把 DHCP 設定好之後，如果想知道 DHCP 分配 IP 位址的情形，可以使用 show ip dhcp binding 指令來查看位址分配列表。執行的範例如下：

```
router#sh ip dhcp binding
IP address     Hardware address    Lease expiration          Type
10.10.1.107 0100.0802.2ec0.75   Mar 02 1993 06:17 AM      Automatic
```

若想將 DHCP 位址分配資料刪除，可使用下列指令：

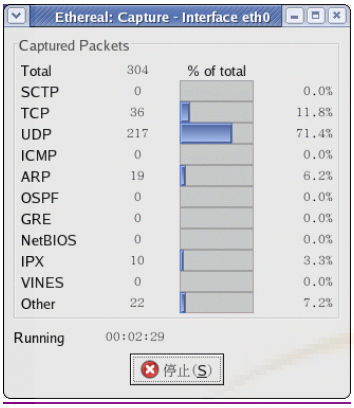
```
Router# clear ip dhcp binding address
```

若想將所有的資料都刪除，也可以執行 clear ip dhcp binding *，系統便會自 DHCP database 中將 DHCP address binding 的資料統統清除。

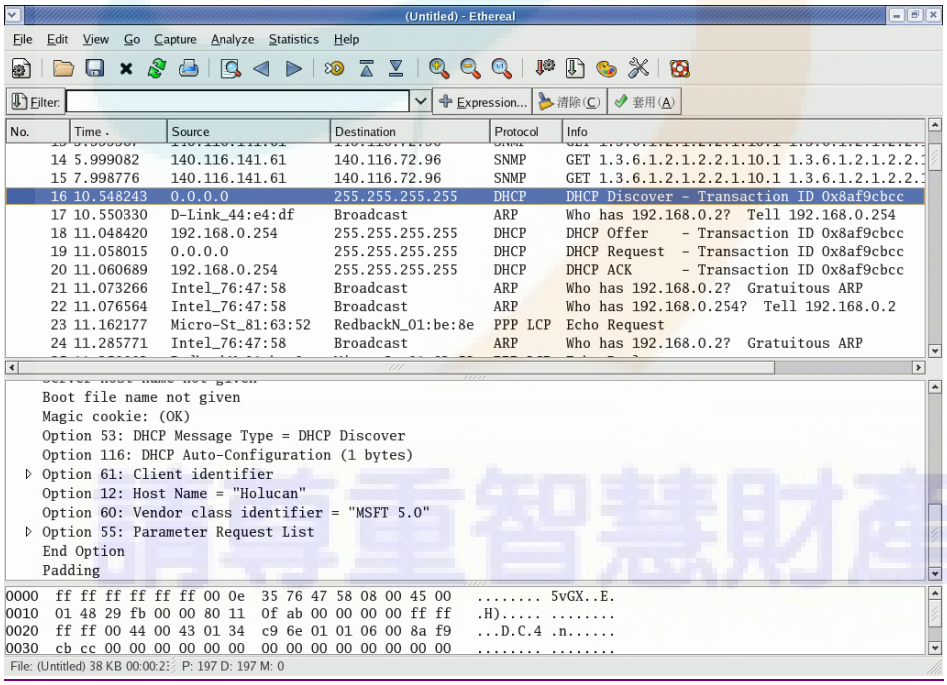
觀察網路上的 DHCP 封包

以下是我們在 Linux 主機 (Fedora) 上，用 Ethereal 擷取到 DHCP 封包的畫面，我們把它列在下面，提供參考。

開始用 Ethereal 擷取網路上的封包...

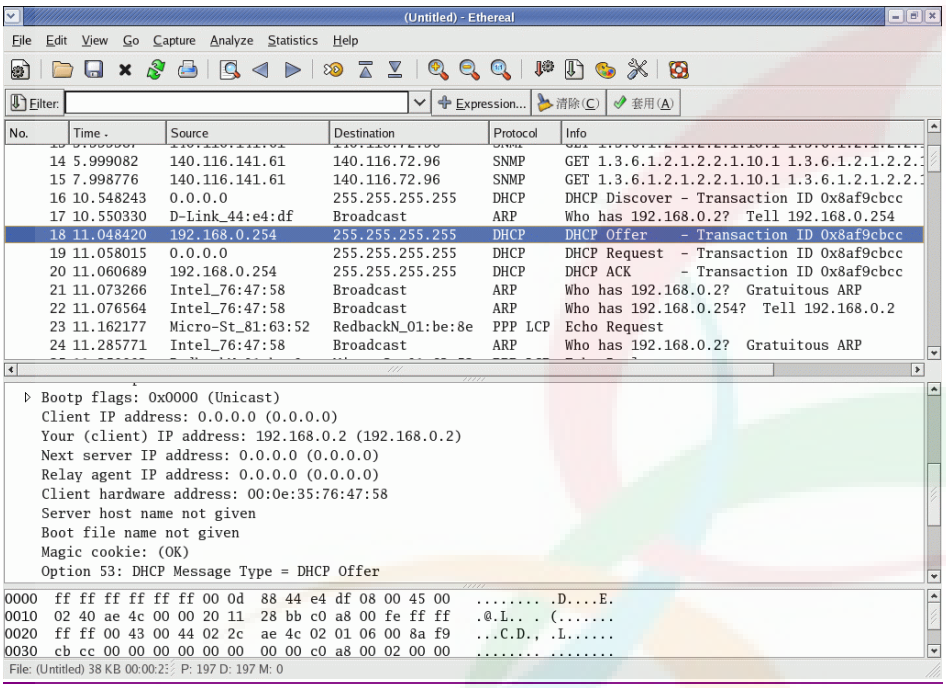


DHCP 搜尋訊息 (DHCP Discover)

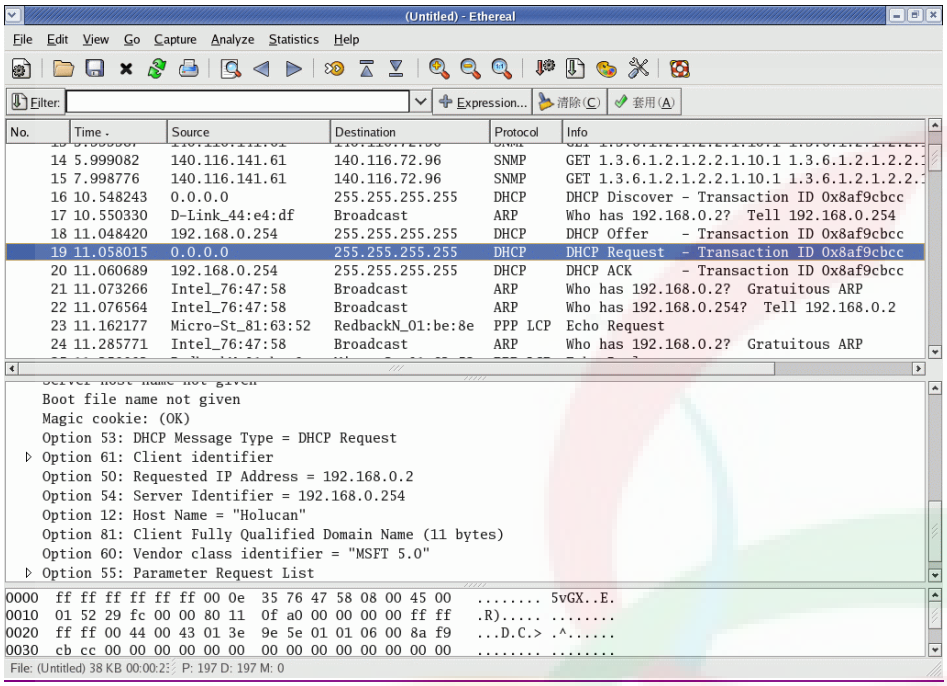


在本例中，Transaction ID 為 0x8af9cbcc

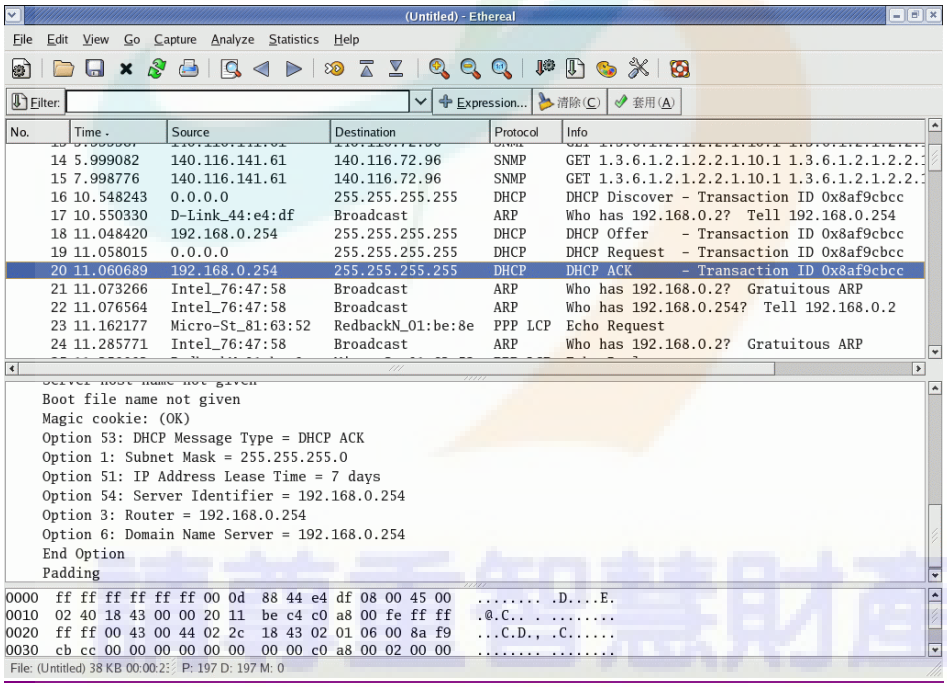
DHCP 伺服器提議訊息 (DHCP Offer)



DHCP 請求訊息 (DHCP Request)



DHCP 回應訊息 (DHCP ACK)



格式化: 字型: (中文) 標楷體

格式化: 左右對齊